



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/521,424	03/08/2000	Satoru Wakao	35.G2550	1497

5514 7590 03/07/2007  
FITZPATRICK CELLA HARPER & SCINTO  
30 ROCKEFELLER PLAZA  
NEW YORK, NY 10112

EXAMINER

HO. THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/07/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/521,424	WAKAO ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Thomas M. Ho	2132	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 11 December 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 38-42, 45-50, 53-58, 61-66 and 69-77 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 38-42, 45-50, 53-58, 61-66 and 69-77 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. Claims 38-41, 42, 45-50, 53-58, 61-66, 69-77 are pending.

#### ***Response to arguments***

2. In response to Applicant's arguments on page 11 of the remarks:

The Examiner contends that the Abstract of 6,209,092 discloses that a watermark may be properly and broadly construed by those of ordinary skill in the art as a One-way function.

The Applicant counters that the relied upon disclosure does not explicitly argue that Natarajan's watermark uses a one-way function. However the burden need not be so high as to necessitate 6,209,092 to reference Natarajan's watermark by name.

What 6,209,092 does is provide further evidence that those of ordinary skill in the art may reasonably construe a digital watermark as a one-way function or using a one-way function, and that such interpretation is not repugnant to the prevailing understanding of the art.

Further arguments in reference to Applicant's amendment regarding the lack of inclusion of encryption using the confidential information are presented below.

*Claim Rejections - 35 USC § 112*

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claim 38-41, along with 42, 45-50, 53-58, 61-66, 69-77 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains new matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicant cites as basis for the new amended claims, (page 2, line 2 of the specification through page 3, line 7). However, it is not clear where it may be explicitly found that a disclosure is made to support the recitation "Wherein the predetermined calculation does not include encryption using the confidential information"

Applicant's (page 2, line 2 of the specification through page 3, line 7) recites a rough outline of the Applicant's entire cryptographic process. Line 9 refers to a digital data M that is hashed to produce item h. h is then processed with a private key to produce s. Is the predetermined calculation M, item h, or s?

It is clear that some confidential information is used to produce to produce the predetermined calculation. In Applicant's arguments of 4/27/2004(page 2), the Applicant argued against the

Art Unit: 2134

Examiner's basis for rejection against the claimed "confidential information" referring to the Examiner's textual information as non-confidential.

However, the only information recited in the portion of the specification recited by the Applicant that may properly serve as confidential information is the private key which is used to produce  $s$  through the use of  $h$ .

It is clear that  $h$  cannot serve as the predetermined calculation because no confidential information is employed to produce  $h$ . The other parameter used to produce  $h$  is the digital data  $M$ .  $H(M) = h$ .  $H$  is not data at all, but a function.

While it appears that the Applicant's digital signature  $s$  may be properly equated with a predetermined calculation produced using confidential information, the use of a private key to produce a signature is in fact a cryptographic process.

For this reason, the Examiner finds Applicant's new amendments lacking support or inconsistent with the specification.

For this reason claims 38-41, along with 42, 45-50, 53-58, 61-66, 69-77, which incorporate the independent claims by reference are rejected under 35 U.S.C. 112 first paragraph.

Art Unit: 2134

To the Examiner's best understanding, the Applicant intended for the amendment of the predetermined calculation to refer to the hash *h*. The Examiner believes this because the Examiner relied upon the encrypted message digest *S* of (item 104, Figure 1) as the predetermined calculation. (Those of ordinary skill in the art understand digest is another term for hash) The portion of the specification the Applicant refers to discloses only a hash without encryption--thus providing the basis for a predetermined calculation not including encryption.

However, this interpretation is not accepted by the Examiner, because it is clear from the basis relied upon the Applicant in the arguments that the hash is not produced with additional confidential information. Only one information parameter is used to compute the hash, Item *M*.

This is significant to the prosecution because it is substantially more burdensome and rare in the art to have a predetermined calculation using *two(emphasis added)* parameters "not including encryption" than just one.

Even more significantly, if the Applicant is allowed to properly call the predetermined calculation, the result of a single parameter hash *h* derived from  $H(M)$ , then Natarajan discloses this nearly word for word (Column 4, line 45-60) & (Figure 1, Message Digest *M*)

For the purposes of advancing prosecution, the Examiner has interpreted the claims not to include the amended limitation "wherein the predetermined calculation does not include encryption using the confidential information".

However, it is noted to the record that if the Applicant desires for the interpretation deriving from the Examiner's best understanding, then Natarajan too discloses that limitation in the alternative in (Column 4, line 45-60) & (Figure 1, Message Digest M)

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 38, 39, 40, 41, 42, 45-47, 50, 53 –55, 58, 61- 63, 66, 69- 70, 73 are rejected under 35 U.S.C. 102(e) as being anticipated by Natarajan, US patent 6611599.

In reference to claim 38:

Natarajan (Figure 1) discloses an apparatus for generating additional data used for checking whether an encoded digital image is changed or not, the apparatus comprising:

- A calculation unit adapted to perform a predetermined calculation using the encoded digital image and confidential information, where the calculation unit is the combination

Art Unit: 2134

of the one way has function unit (Item 100) and the encryption key signature unit (Item 104), and the predetermined calculation is the encrypted message digest, and the confidential information is the private key. (Column 4, lines 60- Column 6, line 25)

- Generating the additional data by applying a one way function to a result of the predetermined calculation, where the generating unit generates(derives) the digital watermark from the encrypted hash. (Item 106) (Column 5, lines 55- Column 6, line 34) & (Figure 1). The Examiner has considered the processing performed by Items 106 et. seq. to derive the digital watermark as elaborated on in (Column 5, lines 55- Column 6, line 34) to be construed as the one-way function that is applied. The provide support for this mapping, US patent 6209092 (abstract) discloses that in the art, the functions used to derive watermark functions may be considered "one-way functions"

*The supplemental information also includes a control pattern, the watermark being generated by applying a one-way function to such control pattern. This has the advantage that any alteration of the watermark or the control pattern can be detected easily, because it is not computationally feasible to calculate a new control pattern for an altered watermark. Therefore, the supplemental information is well protected against unauthorized manipulation. An attempt to fully replace the watermark pattern will affect the quality of reproduction of the content information. In a copy control method allowing a first generation copy ("copy-once"), the original control pattern is processed several times by the one-way function for generating the watermark. Each player or recorder processes the control pattern once before outputting/recording it, thus forming a cryptographically protected down-counter.*

- A recording unit adapted to record the encoded digital image with the additional data on a recording medium, where the recording unit is the apparatus the records the encoded



digital image, and where the information and image that is generated is stored on a recording medium such as a memory or hard drive. (Column 5, lines 55- Column 6, line 25) & (Column 10, lines 45-67)

In reference to claim 39:

Natarajan (Figures 1 & 2) discloses an apparatus for checking whether an encoded digital image is changed or not, the apparatus comprising:

- An inputting unit adapted to input the encoded digital image with first additional data used for checking whether the encoded digital image is changed or not, where the image is detected to see if it has been tampered with. (Column 3, lines 50-63)
- A calculation unit adapted to perform a predetermined calculation using the encoded digital image and confidential information, where the encoded digital image has performed with it, a digital hash to create a message digest, and the confidential information is the private key (Column 4, lines 60- Column 6, line 34)
- generating second additional data by applying a one-way function to a result of the predetermined calculation and a one-way function, where the predetermined calculation is the encrypted message digest(Figure 1), where the second additional data that is generated is the derivation of the digital watermark from the message digest (Column 4, lines 25-52)) & (Column 5, lines 55- Column 6, line 34)
- Wherein said apparatus is adapted to check whether the encoded digital image is changed or not using the first additional data and the second additional data, where the watermark

is used to detect if any changes or tamperings have been made to the digital file and where such detection uses the digital hash and/or watermark. (Column 3, lines 50-63) & (Column 4, lines 25-52)

In reference to claim 40:

Natarajan (Figure 1) discloses a method for use in an apparatus which generates additional data used for checking whether an encoded digital image is changed or not, the method comprising steps of:

- Performing a predetermined calculation using the encoded digital image and confidential information, where the predetermined calculation is the message digest that is encrypted and the confidential information is the private key (Column 4, lines 60- Column 6, line 34)
- Generating the additional data by applying a one-way function to a result of the predetermined calculation and a one-way function, where the additional data generated is the watermark that is derived from the digital hash. (Column 5, lines 55- Column 6, line 34) & (Figures 1 & 2)
- Recording the encoded digital image with the additional data on a recording medium, where the information and image that is generated is stored on a recording medium such as a memory or hard drive. (Column 5, lines 55- Column 6, line 34) & (Column 10, lines 45-67)

In reference to claim 41:

Art Unit: 2134

Natarajan (Figures 1 & 2) discloses a method for use in an apparatus which checks whether an encoded digital image is changed or not, the method comprising the steps of:

- Inputting both the encoded digital image and first additional data used for checking whether the encoded digital image is changed or not, where the inputted additional data is the watermark and digital signature. (Column 4, lines 60- Column 6, line 34)
- Performing a predetermined calculation using the encoded digital image and confidential information, where the encoded digital image has performed with it, a digital hash to create a message digest. (Column 4, lines 25-52) & (Column 5, lines 55- Column 6, line 34)
- Generating second additional data by applying a one-way function to a result of the predetermined calculation and a one-way function, where the second additional data that is generated is the derivation of the digital watermark from the message digest(which is a one way function (Column 4, lines 25-52)) & (Column 5, lines 55- Column 6, line 34)
- Checking whether the encoded digital image is changed or not using the first additional data and the second additional data.

In reference to claim 42:

Natarajan (Figures 1 & 2) discloses an apparatus according to claim 38, wherein the additional data is also used for checking integrity of the encoded digital image, where the integrity of the image is checked with the verification of the digital signature and watermark. (Column 4, lines 60- Column 6, line 34) & (Column 1, line 30 – Column 2, line 26, background of watermarks)

Art Unit: 2134

In reference to claim 45:

Natarajan discloses the apparatus according to claim 38, wherein the confidential information is information unique to the apparatus, where the confidential information is the private key, and the private key is unique to the user and the systems he/she operates. (Column 4, line 60 – Column 5, line 64)

In reference to claim 46:

Natarajan discloses an apparatus according to claim 38, wherein the confidential information is information unique to an external apparatus connected to the apparatus, where the confidential information is the private key, and the private key is unique to the user and the systems he/she operates. (Column 4, line 60 – Column 5, line 64)

In reference to claim 47:

Natarajan discloses an apparatus according to claim 38, wherein the confidential information includes first information unique to the apparatus, and second information unique to an external apparatus connected to the apparatus, where the confidential information is the private key, and the private key is unique to the user and the systems he/she operates, and where the second information unique is the digital signature. (Column 4, line 60 – Column 5, line 64)

In reference to claim 50:

Natarajan discloses an apparatus according to claim 39, wherein the first and second additional data is also used for checking integrity of the encoded digital image, where the first and second

Art Unit: 2134

additional data is the watermark and the digital hash, which are used to check if an image has been tampered with, ie, checking the “integrity” of an image. (Column 1, lines 30 – Column 2, line 26, describing the background and function of digital watermarks) & (Column 2, lines 28-50) & (Column 3, lines 53 – 67) & (Column 4, line 60 – Column 5, line 15)

Claims 53 –55, 58 are substantially similar to claims 45-47, 50 and are rejected for the same reasons as claims 45-47, 50 respectively.

Claims 61- 63, 66 are substantially similar to claims 45-47, 50 and are rejected for the same reasons as claims 45-47, 50 respectively.

Claims 69- 70, 73 are substantially similar to claims 45-47, 50 and are rejected for the same reasons as claims 45-47, 50 respectively.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 48, 49, 56, 57, 64, 65, 71, 72, 74-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Natarajan, US patent 6611599.

Art Unit: 2134

In reference to claim 48:

Natarajan fails to explicitly disclose the apparatus of claim 38, wherein the apparatus is an apparatus which operates as a digital camera but does disclose the apparatus used may be a digital apparatus of some kind. (Column 10, lines 43-67)

The Examiner has taken as admitted prior art that digital cameras was known to those of ordinary skill in the art at the time of invention.

Digital cameras are common consumer devices, the product of a multibillion dollar market.

Advanced cameras such as the Canon 20d, have security features which allow images to indicate if they have been tampered with. This was also the invention of the previously cited art, Friedman US patent 5499294.

It would have been obvious to one of ordinary skill in the art at the time of invention to have the apparatus be a digital camera in order to provide security features for the image in camera, raising security by providing a tamperproof system prior to the image being moved to a computer.

In reference to claim 49:

Art Unit: 2134

Natarajan fails to explicitly disclose the apparatus according to claim 38, wherein the apparatus is an apparatus which operates as a scanner but does disclose the apparatus used may be a digital apparatus of some kind. (Column 10, lines 43-67)

The Examiner takes as admitted prior art that scanners were known to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art at the time of invention to have the apparatus be a digital camera in order to provide security features for the image after it has been scanned to increase security and decrease the opportunity for the image to be tampered with.

Claims 56, 57, 64, 65, 71, 72 are rejected for the same reasons as claims 48 and 49.

In reference to claim 74:

An apparatus according to claim 38, wherein the predetermined calculation includes an exclusive-OR operation.

The Examiner takes official notice that the secure hash algorithm or SHA was well known to those of ordinary skill in the art at the time of invention. SHA is the secure hash algorithm standard designed by NIST along with the NSA for use with the digital Signature Standard. As part of a published government standard for use by the cryptographic community, SHA is employed for federal applications.

SHA in particular discloses a set of nonlinear functions whose computations include the usage of the XOR operation.

It would have been obvious to one of ordinary skill in the art to use SHA and thereby include an XOR operation to adhere to Federal mandate for usage in federal applications.

(See "Applied Cryptography", Schneier, page 442-443 et seq)

Claims 75-77 are rejected for the same reasons as claim 74.

### *Conclusion*

6. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799.

The Examiner may also be reached through email through [Thomas.Ho6@uspto.gov](mailto:Thomas.Ho6@uspto.gov)

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.



Application/Control Number: 09/521,424

Page 16

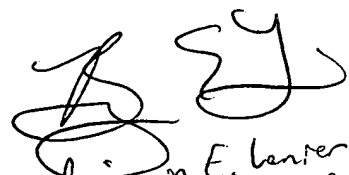
Art Unit: 2134

Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

TMH

March 5<sup>th</sup>, 2007

*Thomas K. AU 2132*

  
Benjamin E. Lerner  
Examiner AU 2132